PHRサービス提供者による健診等情報の取扱いに関する基本的指針（案）に対する意見と回答

●意見募集期間：令和7年3月7日（金）～同年4月7日（月）
●提出意見総数：6件
※提出意見総数は、意見提出者数としています。

No.	資料	該当箇所	意見	回答
1	本体	全体	近年個人情報流失が騒がれている中、個人の健康管理までネット登録する必要はない。どこで悪用されるか、流失になるか不明な状況で、個人リスクが高まるだけ、。政府、医者、一部製薬企業などの利益、利権、利便性、管理、監視しやすいだけの法案は不要です。反対します。	本指針は、PHRサービス提供者が本人同意に基づいて取得した個人情報を適切に利活用するための指針であり、法案ではありません。
2	本体	2.1.(2)③	・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。） P16 D) 通信ネットワークを流れる重要なデータに対して、暗号化等の保護策を実施する ・意見内容 対策のポイントが単に羅列されており、整理が必要かと思われます。下記に意見を列記します。 （意見１） １つ目の対策のＴＬＳと２つ目の対策のＶＰＮはいずれも外部との通信での対策として書かれていますので、ＰＨＲサービスで両方とも対策を実施せよと理解してしまいます。ＴＬＳはユーザがアクセスするとき、ＶＰＮは運用保守で利用すると考えますがいかがでしょうか？ （意見２） ３つ目の健診等情報と４つめの重要なデータやファイルを分けて記述している背景が読み取れません。健診情報も重要なデータやファイルですので「暗号化するなど保護策を講じること」では無く、「暗号化を講じること」にしてはどうでしょうか？ 上記の変更を行うと、電子メールでの送信は、４つ目の対策の事例として記述できます。 （意見３） ４つ目の対策の（例）の最後に「ＰＨＲサービス提供者は・・・」の例が記述されていますが、どのようなことを説明しているのか理解できません。もう少し優しい記述に書き換えていただけると、読者も理解できると思います。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） ございません	（意見１）について、TLSは、PHRサービスユーザー及びPHRサービス提供者の両方によるアクセスに対して通信路の暗号化する対策として求めており、VPNは、PHRサービス提供者による保守運用の際のアクセスでの対策として求めております。 （意見２）について、３つ目の健診等情報に関する記載は、電子メールでのやりとりを想定しており、その対策は暗号化に限らないと言うことを意図しています。４つ目の重要なデータやファイルに関する記載は、一般的な重要なデータファイルに対する暗号化の対策を求めているものです。両記載で意図するものが異なりますので、原案のとおりとさせていただきます。 （意見３）について、御指摘を踏まえ、記載を明確化しました。
3	本体	1.2	意見１ 1ページ 本指針の対象者 本指針の対象者は、利用者に対して、直接的もしくは間接的に健診等情報を取り扱う PHR サービスを提供する者（以下「PHR サービス提供者」という。）とする。 意見 これは、トレーサビリティは確保されているのか。ＰＨＲの情報の不要な拡散を防ぐ情報の流れをすべて把握できるのか。直接的間接的事業者の相関関係などをPHRごとに管理統制できるか	4.2(1)③の「データ提供先の適切性の確認」にて、適切なデータ提供先であることを確認して提供すべき旨記載しており、その中には、本人同意に基づく適切なデータ管理も含まれます。
4	本体	2	意見２ 5ページから25ページ 本指針に基づく遵守すべき事項 情報セキュリティに対する組織的な取り組み 意見２の１ これらのサーバーを海外に置くことに関するリスクは把握されているか ホワイトな人間ばかりでない、最期は信義則に基づき関与するものの誠実性によるため、第3者による監理が必要ではないか 意見２の２ ここまでの規定を設けるためにデジタル化は今後の医療健康に有用なのか デジタルはすでに海外では一周回ってアナログ回帰が進んでいると聞きます。	意見２の１について、本指針では、2.1(2)⑥の「外的環境の把握」にて、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じることを求めております。 意見２の２について、本指針は、安全、安心な PHR（Personal Health Record）サービスの利活用の促進に向けて、PHR サービスを提供する者による PHR の適正な利活用が効率的かつ効果的に実施されることを目的として、PHR サービスを提供する者が遵守すべき事項を示すために策定しているものです。
5	本体	全体	意見３ このＰＨＲ利用事業者及び間接的事業者により個人の人権や生命身体の安全が棄損された場合の救済措置はあるか 現行の関係法令ですべてカバーできるか また、大元のＰＨＲを改ざんさせないための国が統一したセキュリティ対策はあるか大元のデータ改ざん防止は国が対策をとるべきでないか ＰＨＲが様々な関係者の関与を経て話に尾ひれがつくようにならないことが重要	本指針は、安全、安心なPHR（Personal Health Record）サービスの利活用の促進に向けて、PHRサービスを提供する者によるPHRの適正な利活用が効率的かつ効果的に実施されることを目的として、PHRサービスを提供する者が遵守すべき事項を示すために策定しているものです。
6	本体	1.1	民間事業者に個人の保健医療情報を把握されるのは正直言って嫌です。病院等の公的機関のみにしてください。 P.1 健診等情報の具体例として、乳幼児健診、診療情報（なお、薬剤情報、検査情報等も含む）、特定健診等が挙げられる。と書いてありますがこれには遺伝情報も含まれると解釈すると非常に危険ですので辞めてください。 日本政府が個人の保健医療情報を集めて国民の健康を目指し医療費削減を行うとするのは別に構いません。 しかし遺伝情報も含まれると解釈すると非常に危険ですので辞めてください。と私が書いたのは日本に敵対する国に日本国民の保健医療(遺伝情報含む)を把握されてしまったら日本人相手に有効な毒ガス等の生物兵器を開発されるのが非常に恐ろしいです。 この案件はそういった戦争やテロに利用される可能性があるという事を理解してください。	本指針が対象としているPHRサービスは、本人同意に基づいて取得された個人情報に基づいてサービスが提供されるものです。
7	本体	4.2.(1)①	４．２．相互運用性の確保（１） 本指針に基づく遵守すべき事項 １．利用者を介した相互運用性の確保 「データ変換時は互換性を担保するような方式とすること」という記載がありますが、 ・「データ変換」が何を指しているのか ・「互換性」とは何との互換性なのか（マイナポータルAPIから出力される項目及びフォーマットとの互換性でしょうか） といった点が読み取れないため、Q&A等でも補足をいただけますと幸いです。	御指摘を踏まえ、Q&AにQ4-3を追加し、当該記載について補足しました。
8	本体	4.2.(1)③	４．２．相互運用性の確保（１） 本指針に基づく遵守すべき事項 ３．データ提供先の適切性の確認 「データ提供先の PHR サービス提供者の本指針への遵守状況を定期的に確認」とありますが、 この確認方法としてはその前行にある「本指針の別紙チェックシートの確認事項に基づき各要件を満たしていることを確認」 する形でよろしいのでしょうか？ その形でよろしいのであれば、表現をそろえるなどご検討いただけると混乱が少ないかと存じます。	御指摘を踏まえ、確認方法を追記いたしました。
9	本体	1.2	＜項番1＞ ＜該当箇所＞ P1「1.2. 本指針の対象者」のタイトルおよび２行目以下 ＜意見内容＞ 「1.2. 本指針の対象者」を「1.2. 本指針の対象者およびPHRサービスの分類および利用者」とタイトルを変更する。 また、３行目以降に以下を挿入する。 「提供するPHRサービスの内容は以下に分類される。 (1)利用者が主体的に健診等の情報の保存、表示し、予防又は健康づくりおよび診療等に活用できるサービス (2)利用者により保存されたされた情報を委託により加工・分析して利用者に予防又は健康づくりの為のリコメンド並びに医療及び介護現場 で役立てること等を目的としたサービス (3)健診等情報の提供を利用者より受けておこなう同様のサービス (4)上記(1)？(3)のサービスに付帯して複数利用者からの情報の提供を受け情報処理を行うサービス。 (5)上記(1)？(3)のサービスに付帯してサービス提供者が仮名化処理を行って共同研究を行うサービス (6) 上記(1)？(3)のサービスに伴って匿名化処理を行ってサービス提供者が利用又は第三者に提供するサービス また、サービスの利用者は個人情報報の主体者および家族等や医療や介護従事者であり、仮名化処理や匿名化処理を行った場合はPHRサービス提供事業者等も利用者となる。 なお、ガイドラインの中で文脈により利用者・個人・本人・患者が似た意味で用いられているが、それぞれの引用元によるニュアンスを伝えるために統一されていないがほぼ同様の意味で用いられている。」 ＜理由＞ 全体を通してサーボス内容が明確でなく、「３．個人情報の適切な取扱い」での説明を読むと、ＰＨＲサービスの健診等情報の利用主体がサービス提供者のように読めるので、指針の最初で整理した方が良い。	本指針は、PHRサービス全体での遵守事項について定めたものであり、本指針内でPHRサービスの分類を定めるのは自由なサービス創出を阻害する懸念があり適切ではないと思料することから、原案のとおりとさせていただきます。
10	本体	2.1.(2)	＜項番2＞ ＜該当箇所＞ P4 2.1(2) 2行目 ＜意見内容＞ 「リスクアセスメント（リスクの特定・評価・分析）を行い」を 「リスクアセスメント（リスクの特定・分析・評価）を行い」とする。 ＜理由＞ リスクアセスメントの流れの順番に合わせる。	御指摘を踏まえ、修正いたしました。
11	本体	2.1.(2)	＜項番3＞ ＜該当箇所＞ P4 2.1(2) 2行目後半 ＜意見内容＞ 「これらを踏まえたリスク対策 を行う一連のプロセス、すなわち、リスクマネジメントの実施が求められる」を以下に置き換える。 「これらを踏まえたリスク対応に応じた対策およびリスクコミュニケーションを行う一連のプロセス、すなわち、リスクマネジメントの実施が求められる。関連事項は＜1>E」に記述されている。」とする・。 ＜理由＞ ISOや「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」のリスクマネジメントの流れや要求項目及び記述に合わせる。	本指針では、主に一つのサービスを一体的に提供する際のリスク管理を想定しており、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」にあるような、リスクコミュニケーションによる複数者間の合意形成の必要性は想定していないため、原案のとおりとさせていただきます。

12	本体	2.1.(2)①	＜項番4＞ ＜該当箇所＞ P6 2.1(2)＜１＞E)のタイトル ＜意見内容＞ 「情報資産区分に基づいて、リスク管理をすること」を「情報資産区分に基づいて、リスクマネジメントを行うこと」とする。 ＜理由＞ 指針内での用語の統一。JIS Q31000や「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の和訳に合わせる。	御指摘を踏まえ、修正いたしました。
13	本体	2.1.(2)①	＜項番5＞ ＜該当箇所＞ P7 2.1(2)＜１＞E)の3項目目タイトル ＜意見内容＞ 「情報資産のリスク評価に応じた方針を決定し、その方針を実現するための対策を講じること」を 「情報資産のリスク評価に応じたリスク対応を決定し、それを実現するための対策を講じること」とする。 ＜理由＞ ISO31000や「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に合わせる。	当該記載の「方針」は、リスク対応の方針も含むことを意図しておりますので、原案のとおりとさせていただきます。
14	本体	2.1.(2)①	＜項番7＞ ＜該当箇所＞ P7 2.1(2)＜１＞E)の4項目目 ＜意見内容＞ 「情報資産に対するリスク管理を行い、定期的にリスク対策を見直すこと」を 「リスクコミュニケーションを実施し、継続的にリスクマネジメントを行い見直すこと」とする。 ＜理由＞ JIS Q31000や「医療情報を取り扱う情報システム・サービスの 提供事業者における安全管理ガイドライン」に合わせる。	本指針では、主に一つのサービスを一体的に提供する際のリスク管理を想定しており、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」にあるような、リスクコミュニケーションによる複数者間の合意形成の必要性は想定していないため、原案のとおりとさせていただきます。
15	本体	2.2.(1)	＜項番8＞ ＜該当箇所＞ P25 2.2.(1)２行目後半 ＜意見内容＞ 「第三者認証（ISMS 又はプラ イバシーマーク等）を取得することで、客観的に安全管理措置を担保するよう努めなければ ならない。」を以下のような記述にする。 「第三者認証（ISMS 又はプラ イバシーマーク等）を取得することで、健診等情報を取扱うPHRサービス提供者として、最低限の適格性を示すよう努めなければ ならない。 ただし、これら認証の取得をもって、本指針が求める安全管理水準を満たすわけではないことに留意する必要がある。 本指針が求める安全管理に係る評価を行い、評価結果を利用者へ提供する必要がある。 このとき、PHRサービス関連運営業務に関与する担当者自らが評価を行うと、信頼性及び客観性が低下するため、対象PHRサービス提供者内部の独立した監査部門や第三者機関が評価を行うことが望ましい。また、患者等の指示に基づいて医療機関等から医療情報を受領する場合は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン4.3」を踏まえた安全管理に係る評価が求められる。」 ＜理由＞ （ISMS 又はプライバシーマーク評価は情報セキュリティに対する事業者の情報管理体制を評価するもので本指針に沿った安全管理措置を評価するものではない。 こうした評価の目的の違いは、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の4.3及び4.4章に記述されていて、関係者は明確に理解する必要がある。	本指針は、5.1の「本指針の規定する要件を遵守していることの確認」のとおり、要件を遵守していることを自主的に確認し、結果を公表することを基本としています。その上で、マイナポータルAPI経由で健診等情報を入手するPHRサービス提供者においては、第三者認証を取得することを求めております。また、「患者等の指示に基づいて医療機関等から医療情報を受領する場合」については、少なくとも「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の対象となり、当該ガイドラインを参照をいただく旨をQ＆AのQ1-4に記載しております。これらのことから、原案のとおりとさせていただきます。
16	本体	5.1.(1)①	＜項番9＞ ＜該当箇所＞ P34 5.1(1)<1> ＜意見内容＞ 本文の最後に以下を追加する。 「別紙チェックシートの確認結果をホームページに上げる時は安全管理に関する確認が 1)担当者自らの評価 2)独立した監査部門の評価 3)第三者機関の評価であるかを 明記する。 ISMS 又はプライバシーマーク評価を受けている場合はその旨も明示する。 また、患者等の指示に基づいて医療機関等から医療情報を受領する場合は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を踏まえた安全管理の評価を実施している旨も合わせて、1)担当者自らの評価 独立した監査部門の評価3)第三者機関の評価が明確になるように明記する。」 ＜理由＞ ＰＨＲサービス提供者内で乃安全管理の評価意識を向上させるため。評価内容の利用者に対する信頼性を向上させるため。	本指針は、5.1の「本指針の規定する要件を遵守していることの確認」のとおり、要件を遵守していることを自主的に確認し、結果を公表することを基本としています。その上で、マイナポータルAPI経由で健診等情報を入手するPHRサービス提供者においては、第三者認証を取得することを求めております。また、「患者等の指示に基づいて医療機関等から医療情報を受領する場合」については、少なくとも「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の対象となり、当該ガイドラインを参照をいただく旨をQ＆AのQ1-4に記載しております。これらのことから、原案のとおりとさせていただきます。